«Οι επιχειρήσεις και η προσαρμογή στη νέα νομοθεσία για την προστασία προσωπικών δεδομένων»

Σύμφωνα με την πληροφόρηση από το αρμόδιο Υπουργείο Δικαιοσύνης, επίκειται η ψήφιση από τη Βουλή, του νόμου για την προστασία των προσωπικών δεδομένων, ως εφαρμοστικού του Ευρωπαϊκού Κανονισμού όπως ορίζει το ά**ρθρο 1 ΓΚΠΔ/ Άρθρο 1 της Ευρωπαϊκής Οδηγίας 2016/680/ΕΕ.**
Ωστόσο, η νομοθετική ισχύς του Κανονισμού, ούτως ή άλλως, ξεκινά από τις 25 Μαίου και οι συνέπειες μη συμμόρφωσης για όλους, θα επέρχονται κανονικά, μετά την ημερομηνία αυτή. Είναι δηλαδή, ο Κανονισμός αυτός, ανελαστικός, στους κανόνες που επιβάλλει, τόσο στην έναρξη εφαρμογής, όσο και στο κεντρικό πλαίσιο το οποίο παρουσιάζεται μέσα στους αντίστοιχους ρυθμιστικούς κανόνες.

Τι προσωπικά δεδομένα χρησιμοποιούν οι επιχειρήσεις:

Α. Βάσεις δεδομένων του προσωπικού της επιχείρησης. Τηρεί προσωπικά δεδομένα και μάλιστα ευαίσθητα προσωπικά δεδομένα, όπως για παράδειγμα, τον προσωπικό, ιατρικό και οικογενειακό φάκελο του κάθε εργαζόμενου.
Β. Το Μητρώο (στοιχεία) των προμηθευτών.
Γ. Το Μητρώο (τα στοιχεία) των καταναλωτών, πελατών.

Άρα, τρεις βασικές πλατφόρμες, οι οποίες πρέπει να εξεταστούν στο πλαίσιο της ευθυγράμμισης με τον Κανονισμό, δηλαδή η επιχείρηση, με τον κατάλληλο ή με τους κατάλληλους επιστήμονες, συνεργάτες ή με τη βοήθεια του δικηγόρου, να βάλει τους κατάλληλους εκείνους κανόνες, που να την προστατεύσουν όσον αφορά τους εργαζόμενους, τους πελάτες και τους προμηθευτές (υπηρεσίες GDPR).

- Το πρώτο που καλείται να κάνει ένας εξειδικευμένος **επιστήμονας, δικηγόρος ή τεχνικός πληροφορικής,** ή μια εταιρία με τις αντίστοιχες αρμοδιότητες, είναι ένα **scanning της επιχείρησης, των βάσεων δεδομένων,** των εργαζομένων, της κάθετης και οριζόντιας

δομής της επιχείρησης, να δει πώς φυλάσσονται τα αρχεία, με τι τρόπο, με τι εγγυητικές δομές, αν έχει η επιχείρηση συγκεκριμένο τρόπο φύλαξης των αρχείων αυτών κλπ.

Αφού ολοκληρωθεί ουσιαστικά το «σκανάρισμα» το οποίο πρέπει να γίνει στα προσωπικά δεδομένα και αντίστοιχα στις δομές της επιχείρησής σας, κατόπιν αρχίζει και φτιάχνεται, η ανάλυση για τη διασφάλιση των προσωπικών δεδομένων.

Αυτή, θα δώσει ασφαλή αποτελέσματα για τι σημεία πρέπει ουσιαστικά να διορθώσει η επιχείρηση, είτε σε επίπεδο πληροφορικής, είτε σε επίπεδο φύλαξης, είτε σε επίπεδο συμβάσεων. Στις συμβάσεις, θα πρέπει να τοποθετηθούν όροι που να μπορούν να δίνουν τη δυνατότητα στο υποκείμενο των προσωπικών δεδομένων να δηλώσει, εάν επιθυμεί την επεξεργασία ή όχι και με τι τρόπο.

- **Το δεύτερο** είναι να γίνουν τεχνικά, οι κατάλληλες **επεμβάσεις στη μηχανογράφηση της επιχείρησης, ώστε να επιτευχθεί το** υψηλότερο επίπεδο διασφάλισης.
- **Το τρίτο,** είναι, μετά το πέρας αυτής της διαδικασίας, να βγουν ουσιαστικά **οι πολιτικές ασφαλείας**, δηλαδή ένας εσωτερικός Κανονισμός της επιχείρησης, όπου ενσωματώνονται οι συστάσεις και το τι ακριβώς πρέπει να κάνει η επιχείρηση για τη διαφύλαξη των προσωπικών δεδομένων.

Ολοκληρώνοντας τη διαδικασία των πολιτικών διασφάλισης προσωπικών δεδομένων, μπαίνει ο προβληματισμός αν χρειάζονται όλοι DPO ή όχι.

Ο **DPO** είναι **εκείνος, ο οποίος ουσιαστικά θα διασφαλίσει για λογαριασμό του επιχειρηματία, την ευθυγράμμιση της επιχείρησής του, αν δηλαδή, ακολουθεί τους κανόνες** κατά γράμμα, ώστε σε περίπτωση καταγγελίας από εργαζόμενο, είτε από τρίτο, καταναλωτή, πελάτη, **<u>να μπορεί να αποδείξει στην Αρχή Προστασίας Δεδομένων ότι έχει ενεργήσει ορθά και δεν υπάρχουν κενά</u>**. Με λίγα λόγια, η επιχείρηση πήρε μέτρα προληπτικά, διασφαλιστικά, για την προστασία των προσωπικών δεδομένων.

Χρειάζονται όλοι DPO; Η απάντηση είναι όχι. Χρειάζονται μόνο εκείνοι οι οποίοι καταρχήν κάνουν χρήση ευαίσθητων προσωπικών δεδομένων (κλινικές, νοσοκομεία, διαγνωστικά κλπ.), τα Νομικά Πρόσωπα Δημοσίου

Δικαίου, το Δημόσιο, οι παρυφές του Δημοσίου, η κεντρική Κυβέρνηση και καθένας που έρχεται να επεξεργαστεί σοβαρά τα ευαίσθητα προσωπικά δεδομένα.

Άρα: το λιανεμπόριο και τυχόν επιχειρήσεις, οι οποίες κινούνται στη διαδικασία της λεγόμενης «εύκολης, **γρήγορης συναλλαγής, καθημερινής συναλλαγής, εμπορικής συναλλαγής»** και ταυτόχρονα και κάποιες συγκεκριμένες υποκατηγορίες, **δεν χρειάζονται DPO.** Δηλαδή επί της ουσίας ολοκληρώνεται μία διαδικασία μέσα στα πλαίσια της ευθυγράμμισης, στα πλαίσια των υπηρεσιών GDPR (εσωτερικός Κανονισμός της επιχείρησης με τον υπεύθυνο της επεξεργασίας).

Υπάρχουν πιστοποιημένοι DPO; Προς αποφυγή σύγχυσης, παρερμηνείας και κινδύνων εκμετάλλευσης των επιχειρήσεων:

Δεν υπάρχουν αυτή τη στιγμή πιστοποιημένοι DPO. Δεν υπάρχει η διαδικασία πιστοποίησης. Υπάρχουν μόνο κάποια συγκεκριμένα σεμινάρια, τα οποία γίνονται από συγκεκριμένους φορείς, για να μπορούν οι δικηγόροι κυρίως, ή οι υπάλληλοι ή τα στελέχη πληροφορικής ή οι επιστήμονες πληροφορικής, να μπορούν να ανταποκριθούν ευκολότερα.

Ο ΚΑΝΟΝΙΣΜΟΣ ΚΑΙ ΠΟΙΟΥΣ ΑΦΟΡΑ:

Εφαρμόζεται σε κάθε περίπτωση επεξεργασίας, εφόσον το υποκείμενο των προσωπικών δεδομένων ή ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση.

Η μόνη εξαίρεση είναι σε περίπτωση επεξεργασίας προσωπικών δεδομένων για οικιακή, για προσωπική χρήση. Τα τηλέφωνα μέσα στο κινητό, οι επαφές μας, δεν είναι στο πεδίο εφαρμογής του Κανονισμού γιατί είναι για προσωπική χρήση.

Ας μπούμε λίγο στις έννοιες που χρησιμοποιεί και ο Κανονισμός για να καταλάβουμε και το πεδίο εφαρμογής του.

Τι είναι προσωπικά δεδομένα;

Προσωπικά δεδομένα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο Φυσικό Πρόσωπο. Δηλαδή κάθε πληροφορία που, από μόνη της ή σε συνδυασμό και με κάποια άλλη, μπορεί να ταυτοποιήσει ένα πρόσωπο. Είναι το όνομά του, βέβαια. Είναι το τηλέφωνό του. Είναι ο αριθμός κυκλοφορίας του αυτοκινήτου του. Είναι ο αριθμός ΑΜΚΑ, ΑΦΜ,

αριθμός διαβατηρίου. Ακόμη και οι συνήθειες, ότι π.χ. ένας άνθρωπος έχει αυτή τη συγκεκριμένη συνήθεια, ότι κάθε μέρα πάει στο τάδε καφενείο και πίνει καφέ. Είναι προσωπικό δεδομένο, γιατί είναι συνήθεια. Αν μπορούμε δηλαδή να ταυτοποιήσουμε ένα πρόσωπο με μία πληροφορία, τότε αυτή είναι προσωπικό δεδομένο.

Ευαίσθητα προσωπικά δεδομένα θεωρούνται οι πληροφορίες που αφορούν βιομετρικά δεδομένα, γεννητικά δεδομένα, δεδομένα υγείας, δεδομένα για τις σεξουαλικές προτιμήσεις, ποινικές καταδίκες. Αλλά κυρίως είναι τα δεδομένα υγείας.

Επεξεργασία. Τι σημαίνει επεξεργασία; Ακούγοντας τη λέξη, θεωρεί κανένας ότι ως επιχείρηση, κάτι επεξεργάζεστε, κάτι κάνετε με τα προσωπικά δεδομένα. Όχι. Ακόμα μόνο και μόνο που τα τηρείτε σε ένα αρχείο, σε ηλεκτρονικό ή έντυπο, ακόμα και αυτό είναι επεξεργασία. Ακόμα και αν τα διαγράψετε, σας δίνει κάποιος το τηλέφωνό του, το κρατάτε για 5 λεπτά και το διαγράφετε, το σβήνετε, το πετάτε το χαρτάκι και αυτό είναι επεξεργασία προσωπικών δεδομένων. Είναι η συλλογή, η αποθήκευση, η διαγραφή, η διόρθωση, η επικαιροποίηση, είναι τα πάντα που αφορούν τα προσωπικά δεδομένα. Ακόμα και η διαβίβαση, όταν τα δίνετε σε κάποιον τρίτο.

Υπεύθυνος επεξεργασίας. Είναι ένας όρος που τον βρίσκουμε πολύ συχνά μέσα σε όλα τα άρθρα του Κανονισμού. Υπεύθυνος επεξεργασίας, είναι αυτός ο οποίος ορίζει το σκοπό και τον τρόπο της επεξεργασίας. Δηλαδή στην προκειμένη περίπτωση είναι η επιχείρησή σας ο υπεύθυνος επεξεργασίας. Είσαστε εσείς οι ίδιοι ο υπεύθυνος επεξεργασίας. Γιατί, όταν επεξεργάζεστε τα προσωπικά δεδομένα, εσείς ορίζετε και το σκοπό και τον τρόπο της επεξεργασίας.

Εκτελών την επεξεργασία. Ο εκτελών την επεξεργασία, είναι αυτός ο οποίος επεξεργάζεται τα προσωπικά δεδομένα για λογαριασμό σας, για λογαριασμό του υπεύθυνου επεξεργασίας. Για παράδειγμα, όταν δίνετε τα στοιχεία στο λογιστή, για να βγάλει τη μισθοδοσία, αυτός είναι ο εκτελών την επεξεργασία. Κάνει μια δουλειά, μια εργασία, επεξεργάζεται προσωπικά δεδομένα για λογαριασμό σας. Άρα αυτός είναι ο εκτελών την επεξεργασία και λειτουργεί για λογαριασμό σας.

Για να είναι σύννομη η επιχείρησή σας, θα πρέπει να τηρούνται κάποιες αρχές. Να τηρείτε ως υπεύθυνοι επεξεργασίας, κάποιες συγκεκριμένες αρχές.

- **Αρχή διαφάνειας-νομιμότητας**. Ο σκοπός της επεξεργασίας θα πρέπει να είναι νόμιμος. Θα πρέπει να μην επεξεργάζεστε προσωπικά δεδομένα, να μην τηρείτε προσωπικά δεδομένα για σκοπούς που δεν είναι νόμιμοι.

- **Περιορισμός του σκοπού**. Θα πρέπει να επεξεργάζεστε προσωπικά δεδομένα για το συγκεκριμένο σκοπό για τα οποία θέλετε. Δεν έχει νόημα να επεξεργάζεστε προσωπικά δεδομένα τα οποία σας είναι άχρηστα. Δηλαδή, να συγκεντρώνετε προσωπικά δεδομένα για συγκεκριμένο σκοπό, αλλά να μην χρειάζονται αυτά τα δεδομένα. Μόνο αυτά, που χρειάζονται για την επεξεργασία. Αυτό σημαίνει, ότι διατηρείτε όσο το δυνατόν λιγότερα προσωπικά δεδομένα. Αυτά τα δεδομένα επίσης, θα πρέπει να είναι ακριβή και κατά καιρούς να τα επικαιροποιείτε. Να είναι αληθή, να είναι ακριβή. **Αυτό είναι η αρχή της ακρίβειας.**

- **Περιορισμός της περιόδου αποθήκευσης.** Δεν τα κρατάμε επ' αόριστον. Θα πρέπει να τα κρατάτε για τόσο χρονικό διάστημα όσο απαιτείται για την επεξεργασία. Όταν τελειώνει ο σκοπός της επεξεργασίας, ολοκληρώνεται, θα πρέπει αυτά τα δεδομένα να διαγράφονται και να έρχεται και μία συγκεκριμένα διαδικασία διαγραφής τους.

- **Η αρχή της εμπιστευτικότητας**. Θα πρέπει να έχετε όλα τα απαραίτητα μέσα, που διασφαλίζουν την εμπιστευτικότητα των προσωπικών δεδομένων, ότι δεν θα διαρρεύσουν, ότι τα επεξεργάζεστε με ασφάλεια, είτε εσείς, είτε οι υπάλληλοί σας, είτε οι υπεργολάβοι σας, είτε οι εκτελούντες την επεξεργασία για λογαριασμό σας.

Ερώτημα: Εφόσον τηρείτε όλες αυτές τις αρχές, είναι αρκετό και είσαστε σύννομοι; έχετε συμμορφωθεί με τον Κανονισμό; Όχι. Θα πρέπει να δούμε και τι έχει να κάνει στη σχέση σας με το υποκείμενο, με τον φορέα των προσωπικών δεδομένων, με αυτόν που του ανήκουν τα προσωπικά δεδομένα.

Για να είναι σύννομη η επεξεργασία, πρέπει να δούμε και τη σχέση σας με το υποκείμενο, με το φορέα, όπως είπα, των προσωπικών δεδομένων. Άρα για να είναι σύννομη, θα πρέπει να έχετε πάρει τη συγκατάθεση του

υποκειμένου. Ή θα πρέπει να υπάρχει σύμβαση με το υποκείμενο και στο πλαίσιο της εκτέλεσης της σύμβασης αυτής, να μπορείτε να επεξεργάζεστε τα προσωπικά δεδομένα. Οπότε η επεξεργασία αυτή είναι απαραίτητο για τους σκοπούς, για ζωτικό συμφέρον του υποκειμένου.

Αν, λοιπόν, δεν έχουμε τη συγκατάθεση του υποκειμένου, ή αν δεν έχουμε σύμβαση με το υποκείμενο που να μας επιτρέπει την επεξεργασία των προσωπικών δεδομένων, τότε δεν είναι και σύννομη η επεξεργασία μας. Υπάρχουν, βέβαια, και εξαιρέσεις.

Με τον εργαζόμενο έχω σύμβαση, επομένως δεν έχει νόημα να πάρω τη συγκατάθεσή του. Ούτως ή άλλως, και από τον Κανονισμό, αυτό εξαιρείται. **Αυτό δεν σημαίνει όμως ότι δεν θα έχω και τα απαραίτητα μέτρα** που θα διασφαλίζουν ότι η επεξεργασία των προσωπικών του δεδομένων γίνεται με τρόπο ασφαλή. Θα πρέπει να έχω πολιτικές που διασφαλίζουν την επεξεργασία, όπως προβλέπεται στον Κανονισμό.

Το ίδιο συμβαίνει και με τα ευαίσθητα προσωπικά δεδομένα, που αφορούν την υγεία. Ευαίσθητα προσωπικά δεδομένα, απαγορεύεται με βάση τον Κανονισμό να τύχουν αντικειμένου επεξεργασίας, από τον υπεύθυνο επεξεργασίας. Θα πρέπει μόνο όταν έχουν τη συγκατάθεση του υποκειμένου. Μόνο τότε θα μπορείτε να επεξεργάζεστε ευαίσθητα προσωπικά δεδομένα.

ΠΩΣ ΠΑΙΡΝΕΤΕ ΤΗ ΣΥΓΚΑΤΑΘΕΣΗ:

Η συγκατάθεση, που θα πρέπει να πάρετε από τον υπάλληλό σας ή από τον πελάτη σας, θα πρέπει να είναι έγγραφη και να μπορείτε να το αποδείξετε σε οποιοδήποτε τρίτο θα έρθει να σας κάνει έλεγχο, ότι είχατε πάρει τη συγκατάθεση του υποκειμένου για να μπορέσετε να επεξεργαστείτε προσωπικά του δεδομένα.

Αυτό, στην πράξη θα είναι ή μέσα στη σύμβαση. Θα είναι ένας επιπλέον όρος μέσα σε μία σύμβαση που μπορεί να έχετε, ή θα είναι ένα ξεχωριστό και αυτό συμβουλεύουν και η Αρχή Προστασίας Δεδομένων, για να είναι ξεκάθαρο και στον αντισυμβαλλόμενό σας τι υπογράφει. Να είναι ξεχωριστό έντυπο, στο οποίο θα αναφέρονται οι σκοποί, για ποιο σκοπό θα επεξεργαστείτε τα προσωπικά του δεδομένα.

Παράδειγμα: παίρνετε το e-mail του: «*Θα χρησιμοποιήσω το e-mail σου, για να σε ενημερώνω γι' αυτό, για να σου στέλνω προωθητικές ενέργειες, για να*

διαφημίσω την επιχείρησή μου. Θα χρησιμοποιήσω το κινητό σου τηλέφωνο γι' αυτό το λόγο»…..

Θα πρέπει να αναφέρονται δηλαδή, ένας προς έναν, οι σκοποί. Αν προστεθεί κάποιος καινούργιος σκοπός, θα πρέπει να ανανεωθεί το έντυπο πάλι. **Δεν μπορούμε δηλαδή να προσθέτουμε μόνοι μας σκοπούς, αν δεν έχουμε πάρει τη συγκατάθεση την προηγούμενη του υποκειμένου**. Άρα πρέπει, η συγκατάθεση να είναι ένα βήμα πριν, από τη χρήση των προσωπικών δεδομένων.

Στην πράξη, θα πρέπει στους πελάτες σας, να έχετε στείλει ένα χωριστό mail, αν κρατάτε mail, αν η επικοινωνία σας γίνεται με αυτό τον τρόπο και ο αποδέκτης σας (πελάτης, κ.λπ) να απαντήσει, ότι ουσιαστικά αποδέχεται, εγκρίνει τις ενέργειές σου. Π.χ: «ναι, αποδέχομαι να κάνεις χρήση του mail μου, για να μου στέλνεις το προωθητικό σου υλικό το διαφημιστικό, να μου στέλνεις εκπτωτική ύλη, να μου στέλνεις κάτι άλλο που εσύ πιστεύεις σημαντικό στα πλαίσια του marketing και της διαφήμισης». **Αν σου πει ο πελάτης «όχι», δεν δικαιούσαι να τον ενοχλήσεις με ο,τιδήποτε είναι αυτό.**

Συμπερασματικά

Τι ακριβώς περιμένει ο Κανονισμός να κάνετε εσείς;

Πρώτον, θα πρέπει να έχετε πάρει τη συγκατάθεση από το υποκείμενο, όπως είπαμε προηγουμένως, με τρόπο που μπορείτε να το αποδείξετε.

Δεύτερον, θα πρέπει να έχετε ενημερώσει το υποκείμενο των προσωπικών δεδομένων, τον πελάτη σας, για τα δικαιώματά του εγγράφω, στο ίδιο έντυπο που μπορεί να παίρνετε και τη συγκατάθεση, ότι «αυτά είναι τα δικαιώματά σου, δίνεις τη συγκατάθεσή σου, γιατί αυτό είναι υποχρέωση που πηγάζει από τον Κανονισμό». Ακόμα και για το δικαίωμά του ότι μπορεί να σας καταγγείλει, θα πρέπει να τον έχετε ενημερώσει και γι' αυτό ακόμα, ότι μπορεί να σας κάνει καταγγελία για κάποια παράβαση των προσωπικών δεδομένων.

Θα πρέπει να τον ενημερώνετε για ποιους σκοπούς συλλέγετε τα προσωπικά του δεδομένα, για να του στείλετε π.χ. ένα προωθητικό υλικό, για πόσο

χρόνο τα κρατάτε και γενικά θα πρέπει να τον ενημερώσετε για την επεξεργασία των προσωπικών του δεδομένων. Δηλαδή αν τα δίνετε σε κάποιον τρίτο ή όχι, όλα αυτά θα πρέπει να είναι ενήμερο το υποκείμενο.

Τρίτον, θα πρέπει να έχετε μία πολιτική, όπως στο ISO, που υπάρχουν διαδικασίες, έτσι και εδώ, θα πρέπει να έχετε μία διαδικασία για την επεξεργασία των προσωπικών σας δεδομένων, ένα εγχειρίδιο, για το πώς θα επεξεργάζεστε τα προσωπικά δεδομένα. Αυτό, θα είναι σαν «ευαγγέλιο» της επιχείρησής σας, γιατί μ' αυτό, όταν τυχόν ελεγχθείτε, θα μπορείτε να αποδείξετε ότι, όντως, υπάρχει ασφαλής επεξεργασία προσωπικών δεδομένων.

Τέταρτον, η τελευταία σας υποχρέωση, είναι **να εκπαιδεύσετε τους υπαλλήλους σας, το προσωπικό σας** και όποιους τρίτους, με τους οποίους συνεργάζεστε. Αν έχετε κάποιον τρίτο, στον οποίο διαβιβάζετε τα προσωπικά δεδομένα, όπως το λογιστή σας, με αυτόν πρέπει οπωσδήποτε πλέον να έχετε έγγραφη σύμβαση. Είναι ρητή υποχρέωση με βάση τον Κανονισμό. Αν δεν έχετε σύμβαση, πρέπει να την κάνετε μόνο και μόνο για τα προσωπικά δεδομένα, με συγκεκριμένες διατάξεις, με συγκεκριμένα άρθρα.

ΕΝΗΜΕΡΩΣΗ:

Το Β.Ε.Α. πέραν της διαρκούς γενικής ενημέρωσης που θα παρέχει για το θέμα, μέσω της ιστοσελίδας και των υπηρεσιών του, προκειμένου να υποστηρίξει έμπρακτα τις επιχειρήσεις – μέλη του, καθώς και τις συνδικαλιστικές οργανώσεις των κλάδων που εκπροσωπούνται σε αυτό, δρομολογεί την εξειδικευμένη πληροφόρηση και υποβοήθηση, στη διαμόρφωση κανονισμού συμμόρφωσης των επιχειρήσεων.

Στο προσεχές διάστημα, θα δημοσιευτεί η αναλυτική ενημέρωση για τις δράσεις του Επιμελητηρίου.